Lab 276

Morris & Opazo

aws re/start

Endurecimiento de la red

INTRODUCCIÓN

Amazon Inspector realiza análisis de todas sus configuraciones de red, como grupos de seguridad, listas de control de acceso de red (ACL de red), tablas de ruta y gateways de Internet, juntas para inferir la accesibilidad. No necesita enviar paquetes a través de la red de nube virtual privada (VPC) o conectarse a los puertos de red de una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Es como un mapeo y reconocimiento de red sin paquetes.

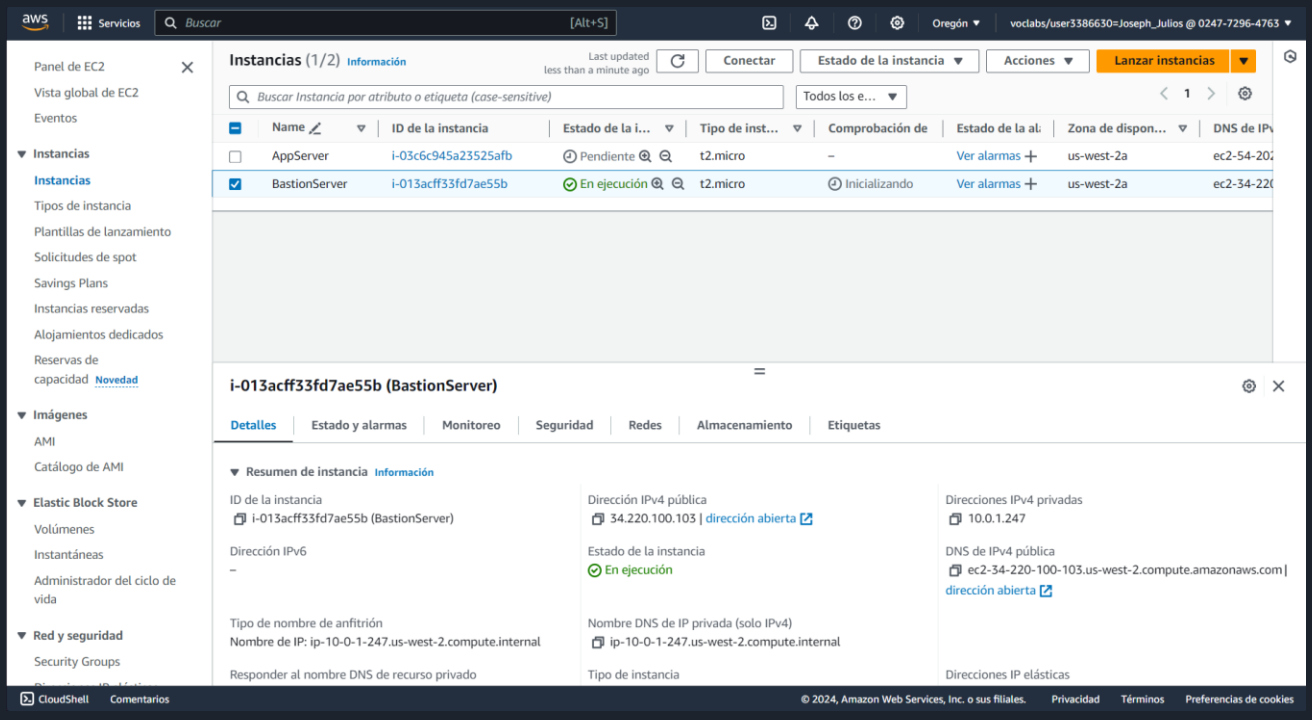
OBJETIVOS

- Configurar Amazon Inspector.
- Ejecutar una auditoría de red sin agente.
- Investigar los resultados del análisis.
- Actualizar grupos de seguridad.
- Inicie sesión en una estancia del servidor de aplicación usando AWS Systems Manager Session Manager.

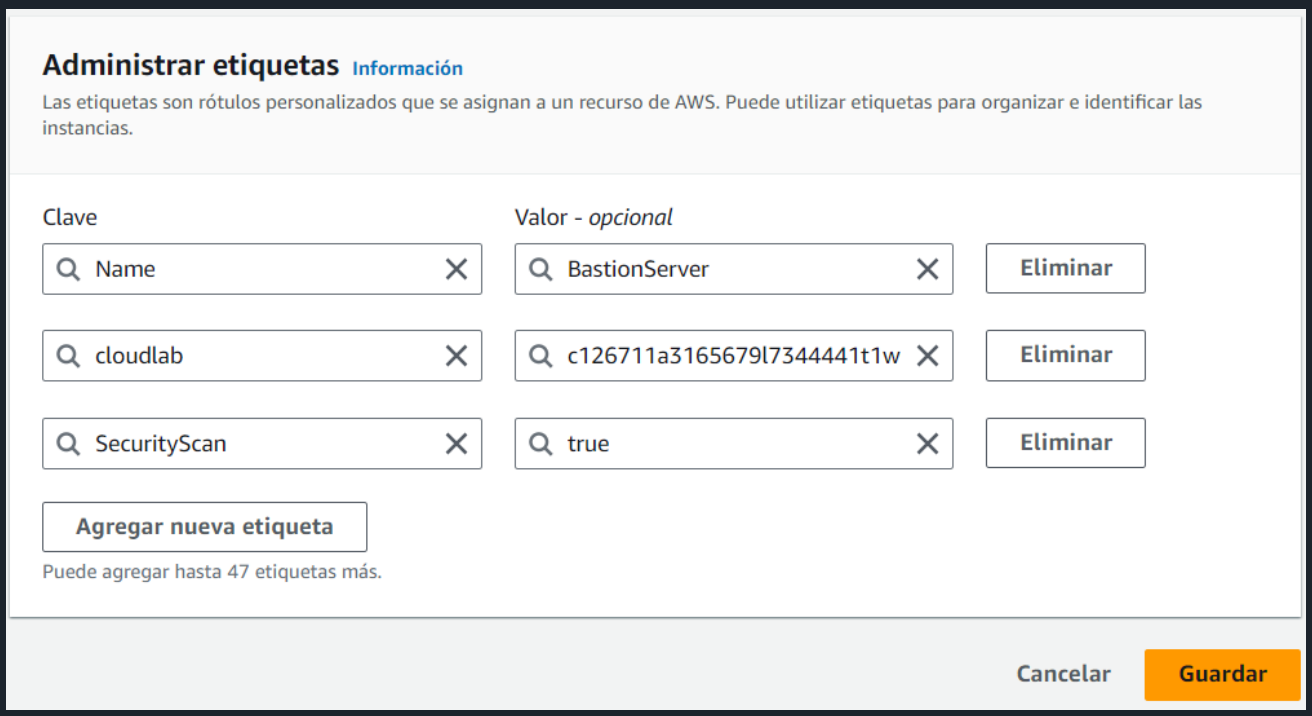
TAREA 1

Para crear un objetivo de evaluación para Amazon Inspector Classic para evaluar, debe comenzar por etiquetar las instancias de EC2 que desea incluir en su objetivo. En esta tarea, etiquetará la instancia de BastionServer.

- En la Consola de administración de AWS, seleccione Services (Servicios) y seleccione EC2.
- En el panel de navegación izquierdo, elija Instances.
- Seleccione la instancia de BastionServer.



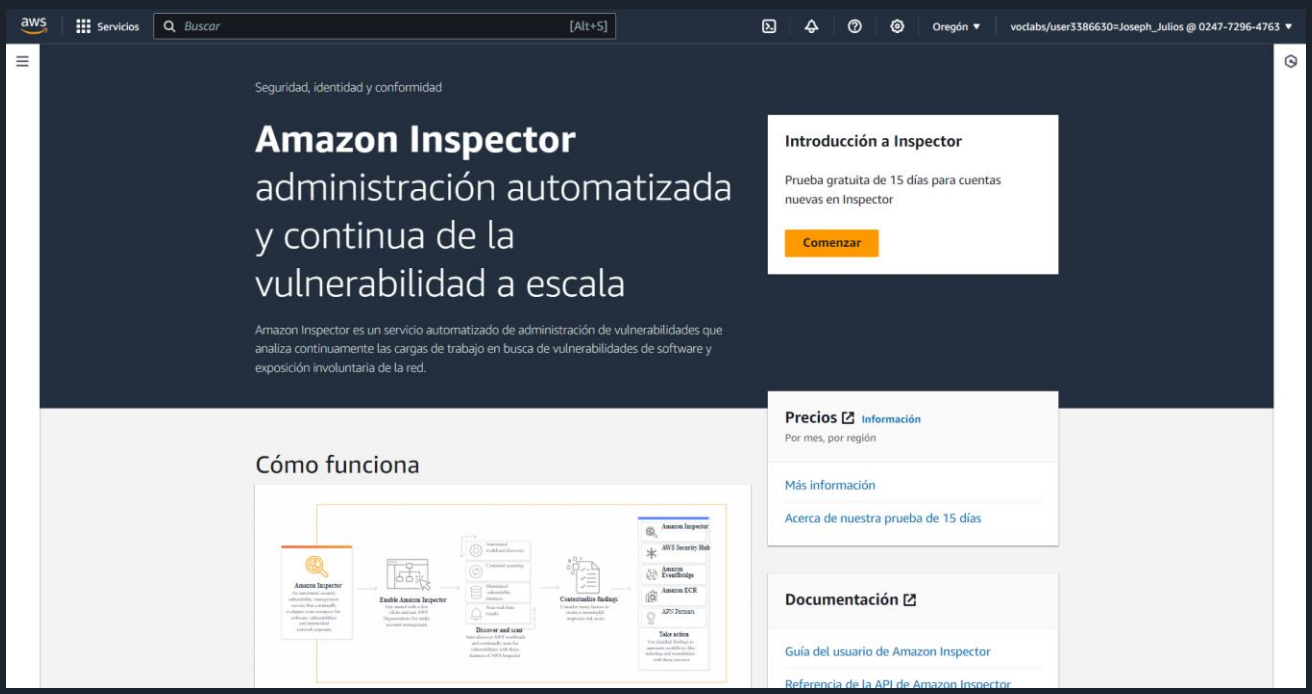
- Seleccione la pestaña Tags (Etiquetas).
- Seleccione Manage Tags (Administrar etiquetas).
- Seleccionar la pestaña de etiquetas, administrar etiquetas y agregar la información. Seleccione guardar.



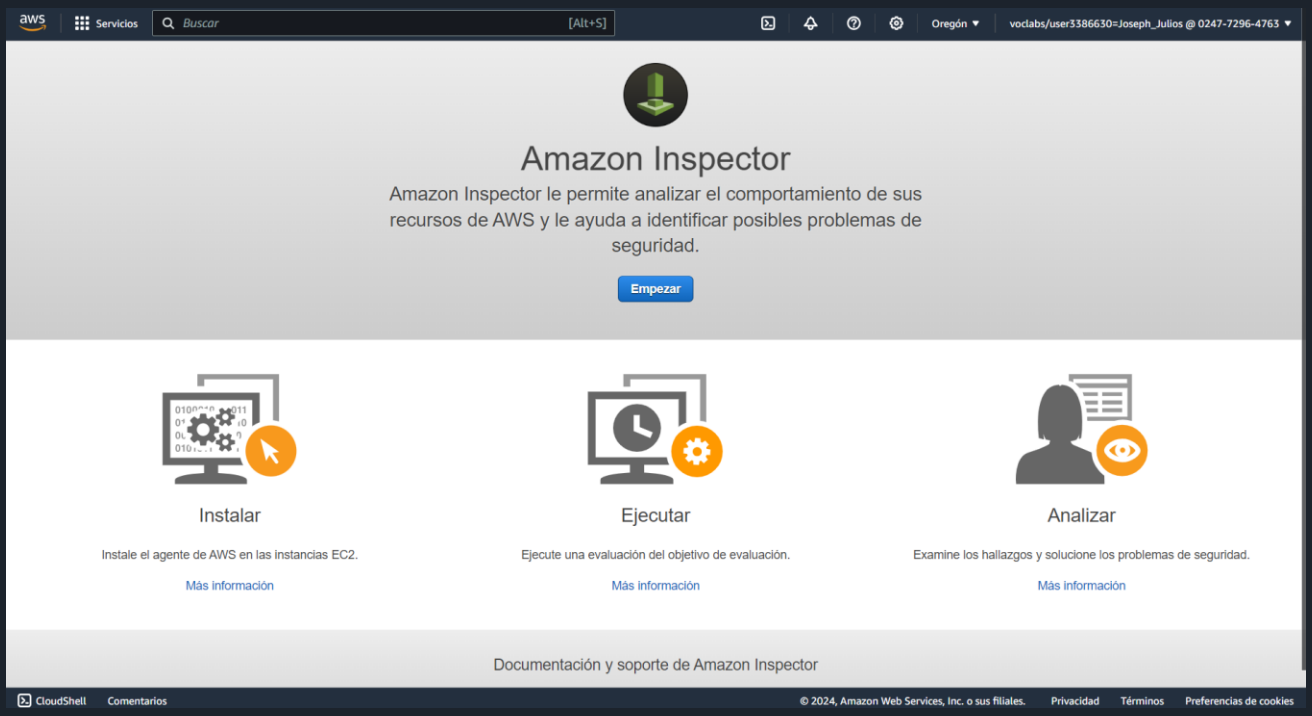
TAREA 2

En esta tarea, aprenderá a ejecutar una auditoría de red sin agente en sus instancias de EC2 usando Amazon Inspector. Para este laboratorio, usará el paquete de reglas de accesibilidad de red.

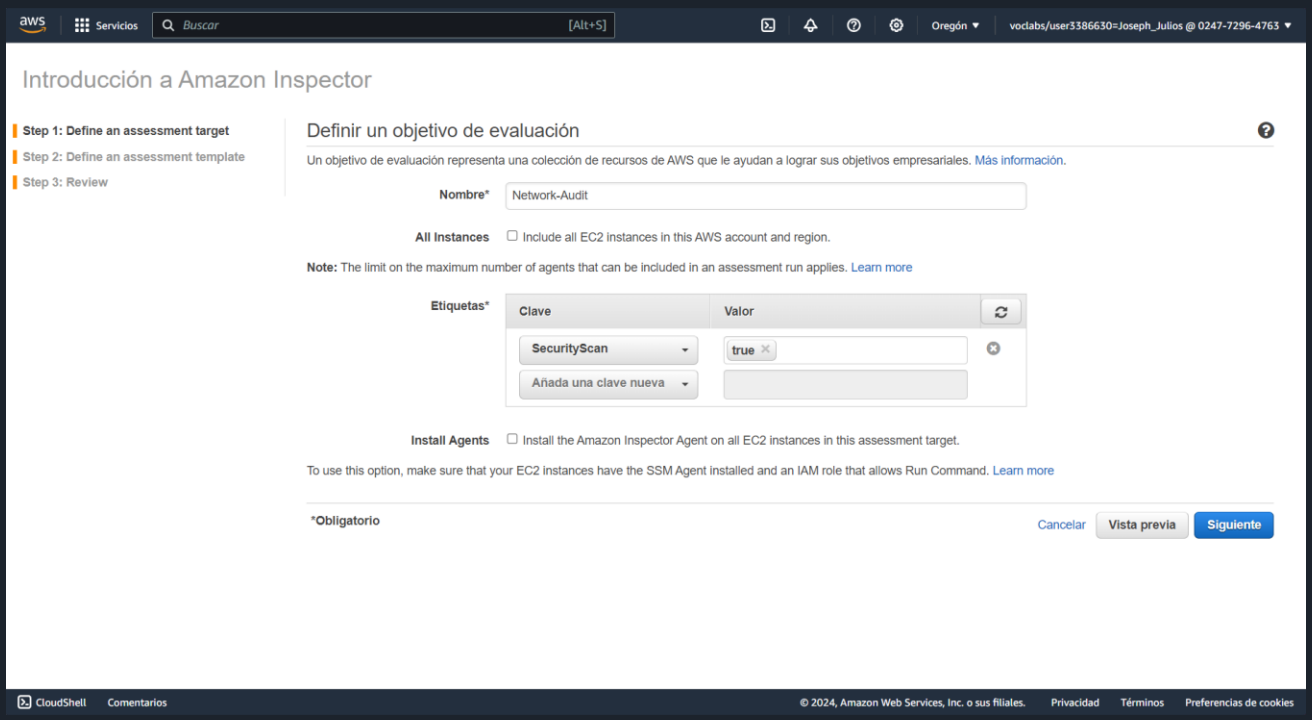
- Seleccionar el servicio Inspector en el apartado de servicios.



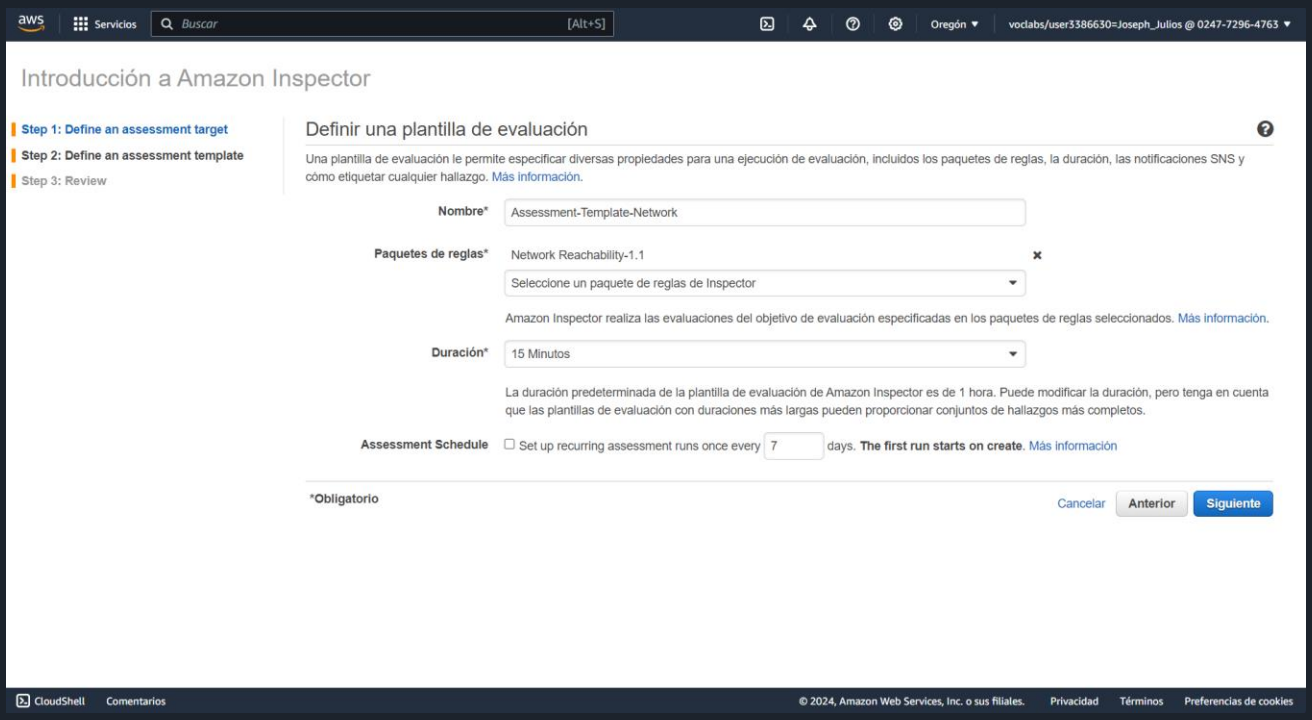
- Seleccione Switch to Inspector Classic (Cambiar a Inspector Classic).



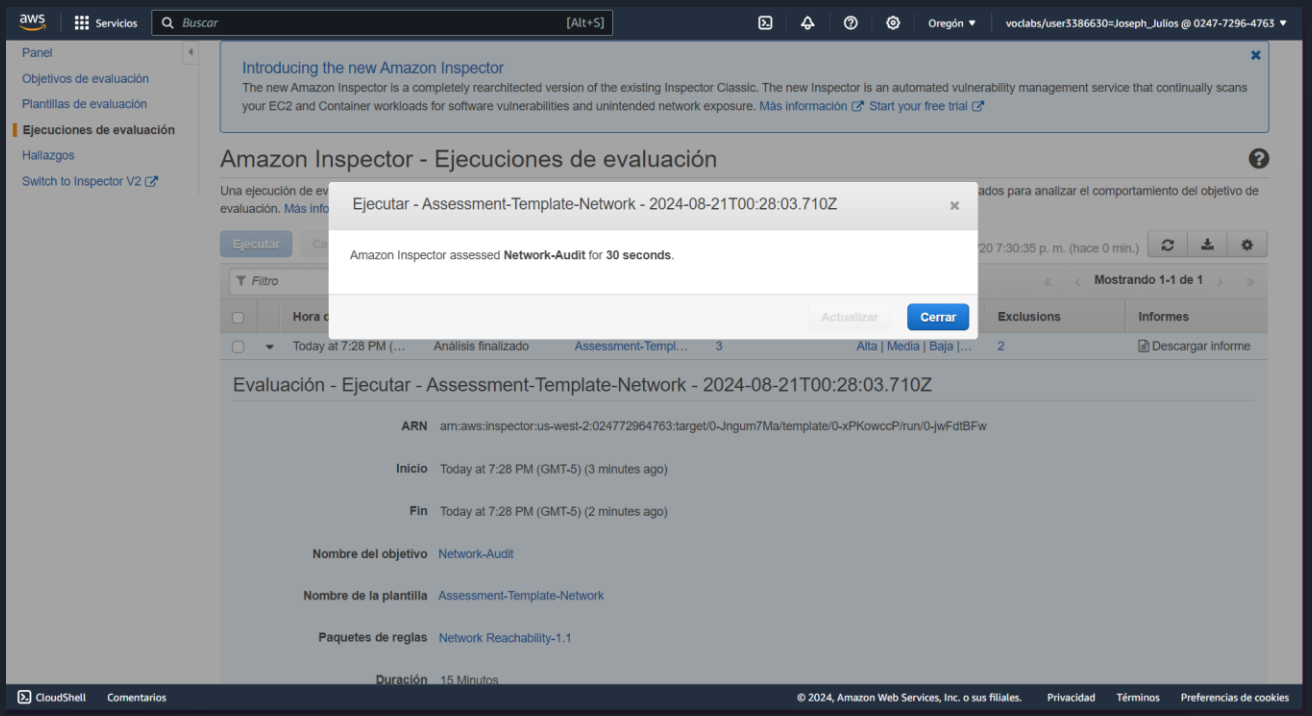
- Seleccione Get Started.
- Seleccione Advanced setup.
- Configurar la sección de Definir un objetivo de evaluación.



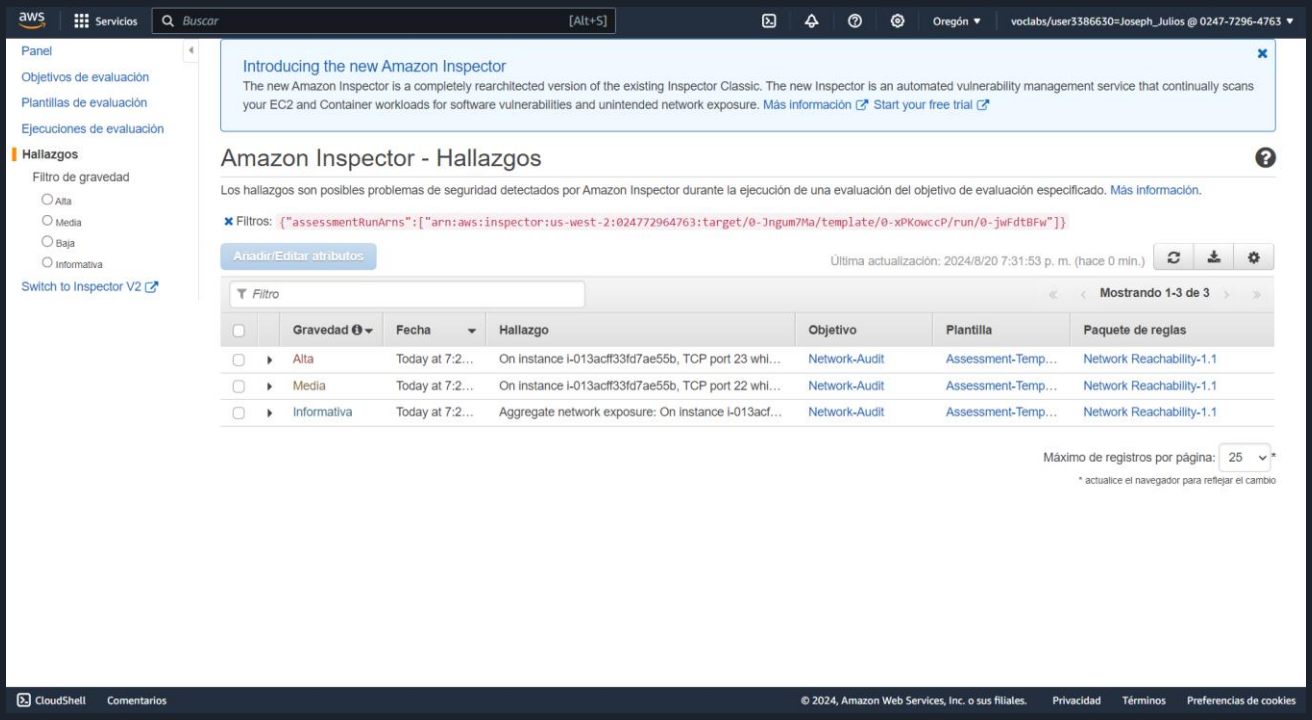
- Configurar la sección de Definir una plantilla de evaluación.



- Verificar el estado del análisis.



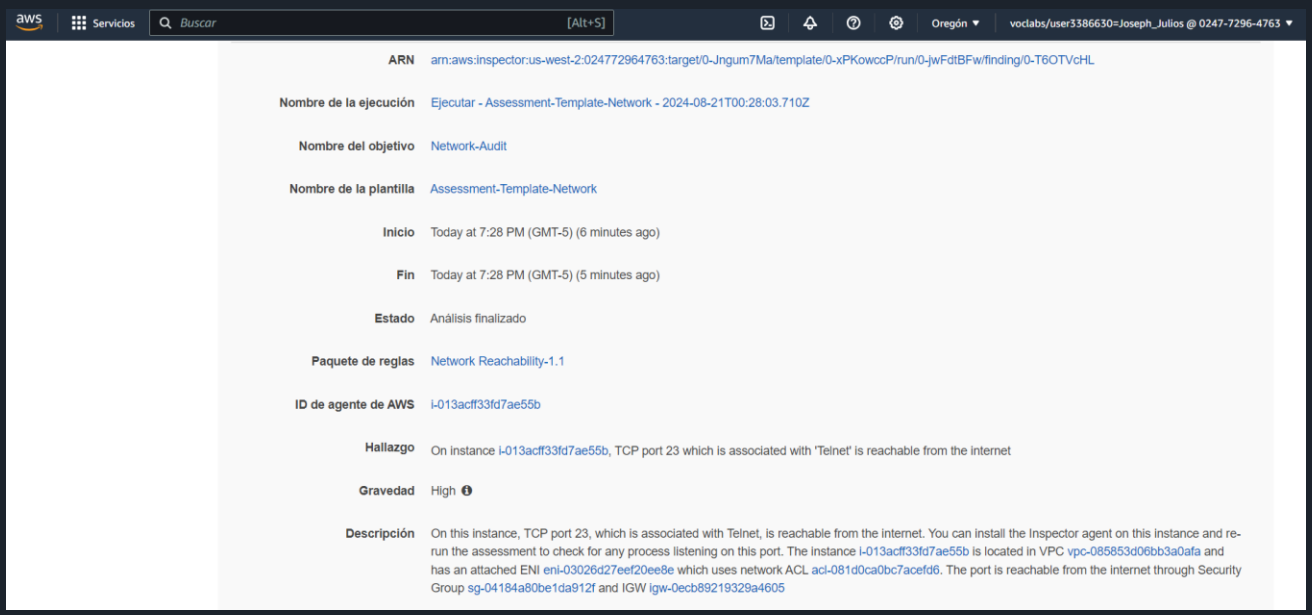
- Cuando el estado cambie a Analysis complete, seleccione Findings en el panel de navegación.



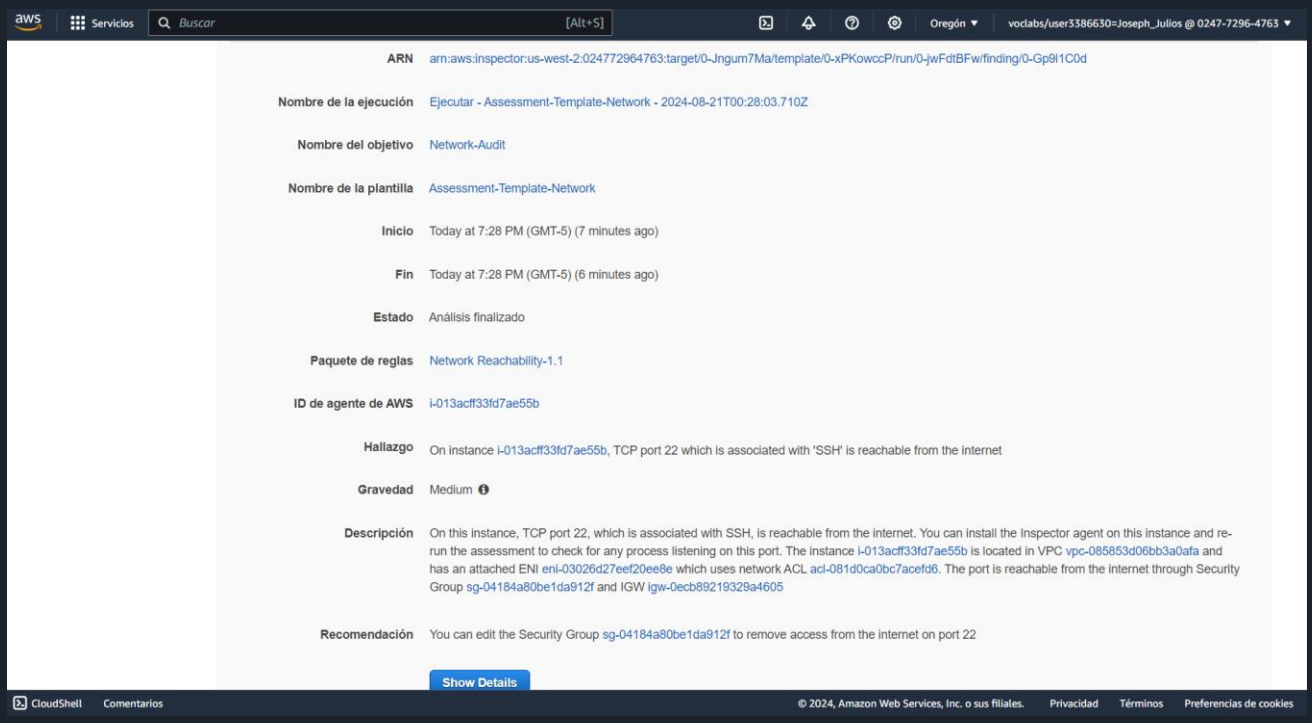
TAREA 3

Los hallazgos que esas reglas generan muestran si sus puertos son accesibles desde Internet mediante un gateway de Internet (incluidas instancias detrás de equilibradores de carga de aplicación o equilibradores de carga clásicos), una interconexión de VPC o una red privada virtual (VPN) mediante un gateway virtual. Estos hallazgos también destacan las configuraciones que permiten potenciales accesos maliciosos, como grupos de seguridad, ACL y gateways de Internet mal administrados.

- Revisar el hallazgo de alta severidad. Debería poder ver los siguientes detalles clave.



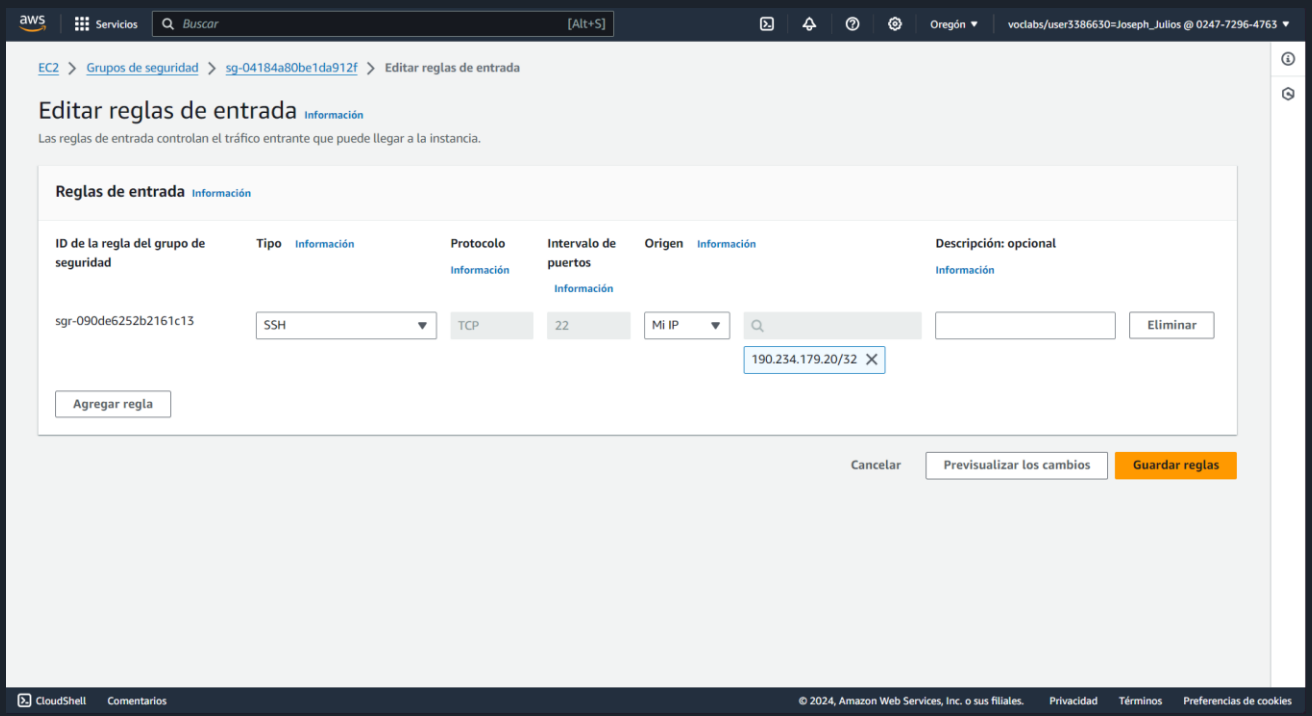
- Revisar los hallazgos de severidad media y analizar los detalles.



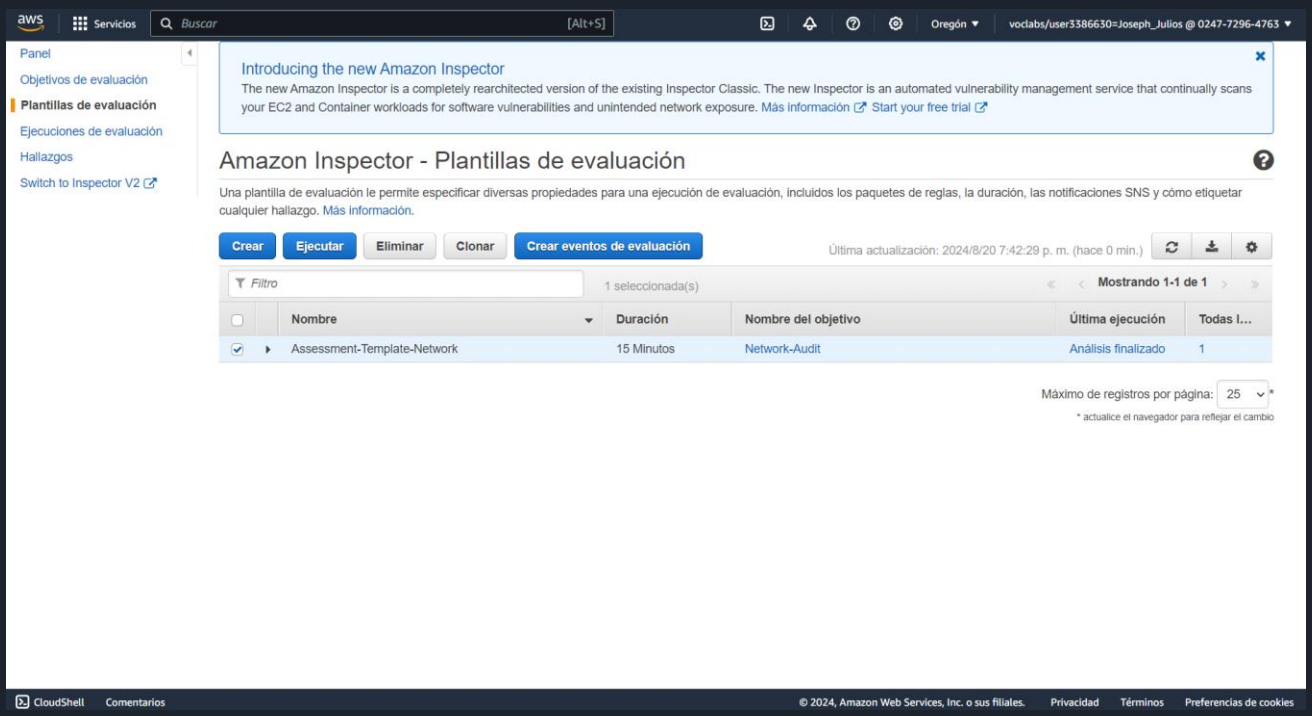
TAREA 4

En esta tarea, verá algunas opciones de corrección para los hallazgos de seguridad que Amazon Inspector detectó. La primera opción muestra cómo bloquear el puerto 22 para direcciones IP específicas.

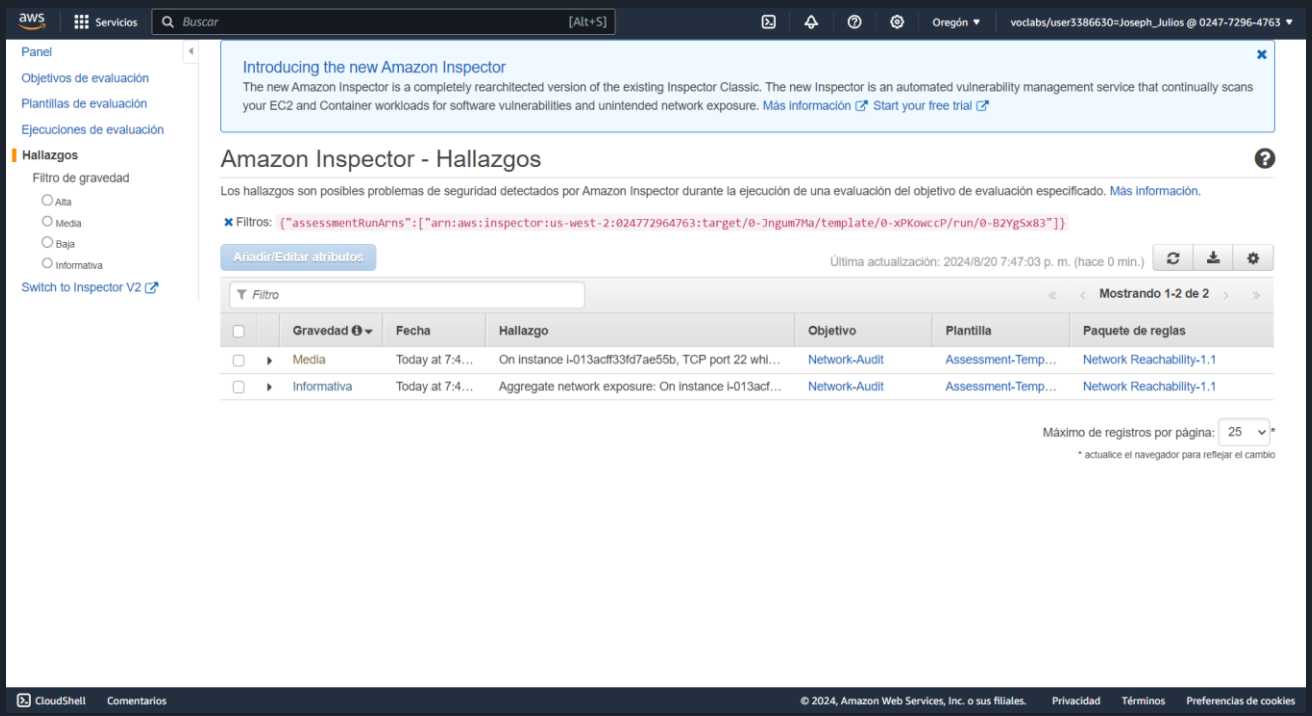
- Revisar los detalles del hallazgo de alta severidad.
- Seleccionar el enlace para el grupo de seguridad. Los enlaces deben ser similares al siguiente ejemplo: sg-0b2dc685cd6e6e706.
- Editar las reglas de entrada.



- Ejecutar la plantilla de evaluación Assessment-Template-Network.



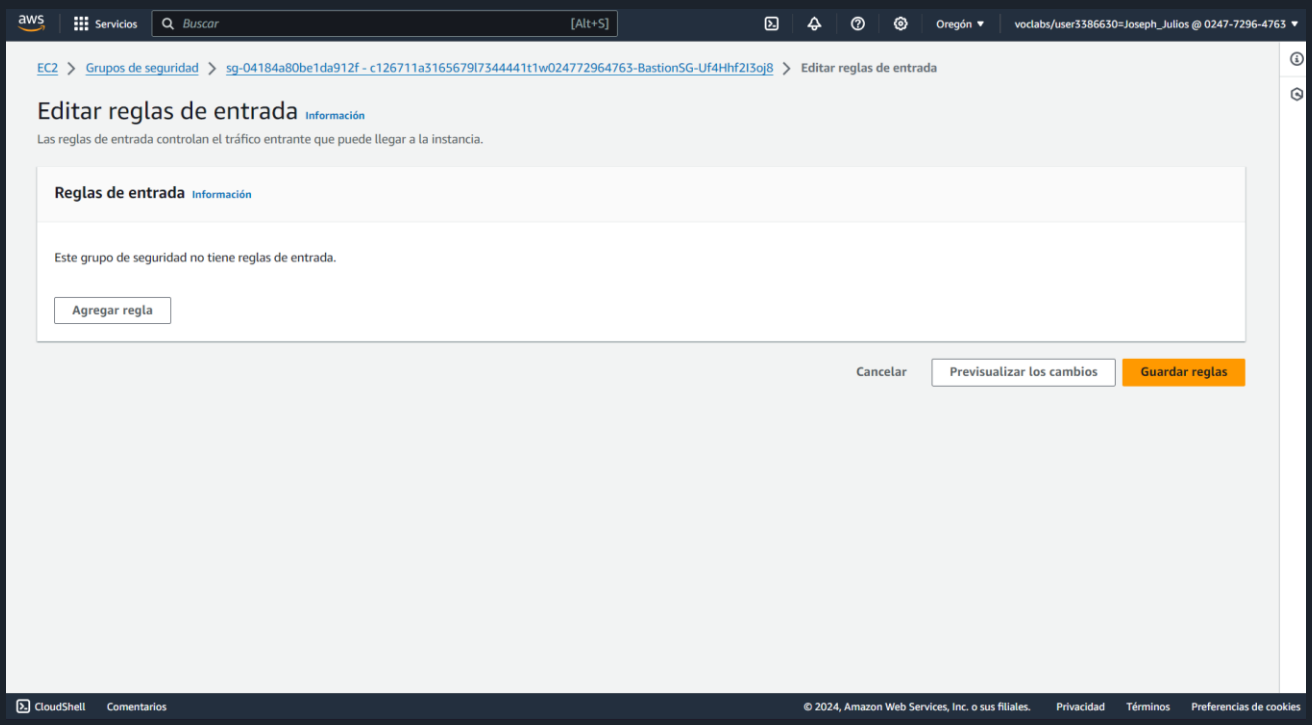
- Seleccionar Ejecuciones de evaluación.
- Revisar los hallazgos y seleccionarlos según fecha.



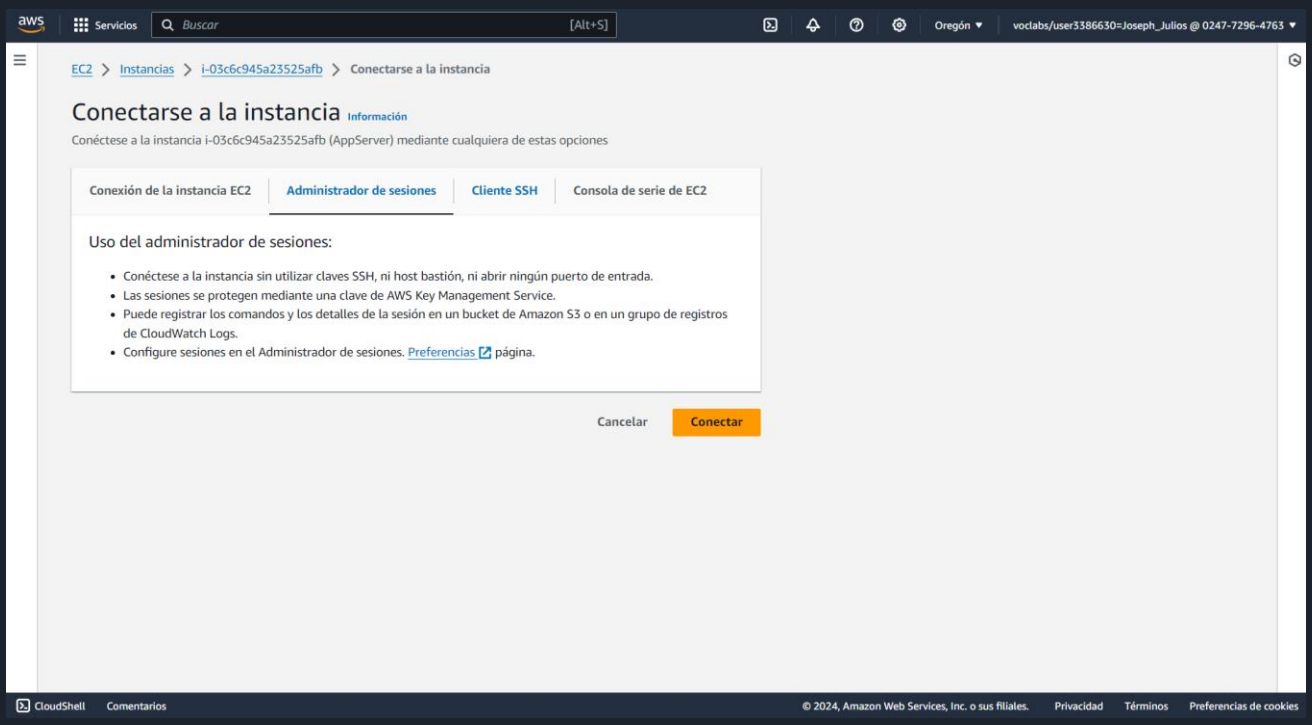
TAREA 5

En esta tarea, reemplazó la instancia de BastionServer, que usaba principalmente SSH para conectarse a AppServer dentro de la subred privada. En su lugar, usted usa Session Manager mediante Systems Manager.

- Ubicarse en el servicio EC2 de AWS, en el apartado de grupo de seguridad.
- Editar reglas de entrada para BastionServerSG, eliminar la regla de entrada de SSH.



- Detener instancia BastionServer.
- Conectarse mediante Session Manager a App Server.



- Análisis final, ejecutar evaluación y revisar los detalles de los hallazgos.

- Vaya a la pestaña del navegador que tiene Amazon Inspector abierto.

- En el panel de navegación izquierdo, elija Assessment runs (Ejecuciones de evaluación).
- Seleccione la casilla para la evaluación ejecutada anteriormente y luego seleccione Run (Ejecutar).
- Espere que Status (Estado) muestre Analysis complete (Análisis completo) y seleccione para expandir los detalles de la ejecución de evaluación más reciente.
- Compruebe que no haya ningún Hallazgo.